

TECHNOLOGY / ON-LINE / POLITICS

Techie alert: Even you can be hacked

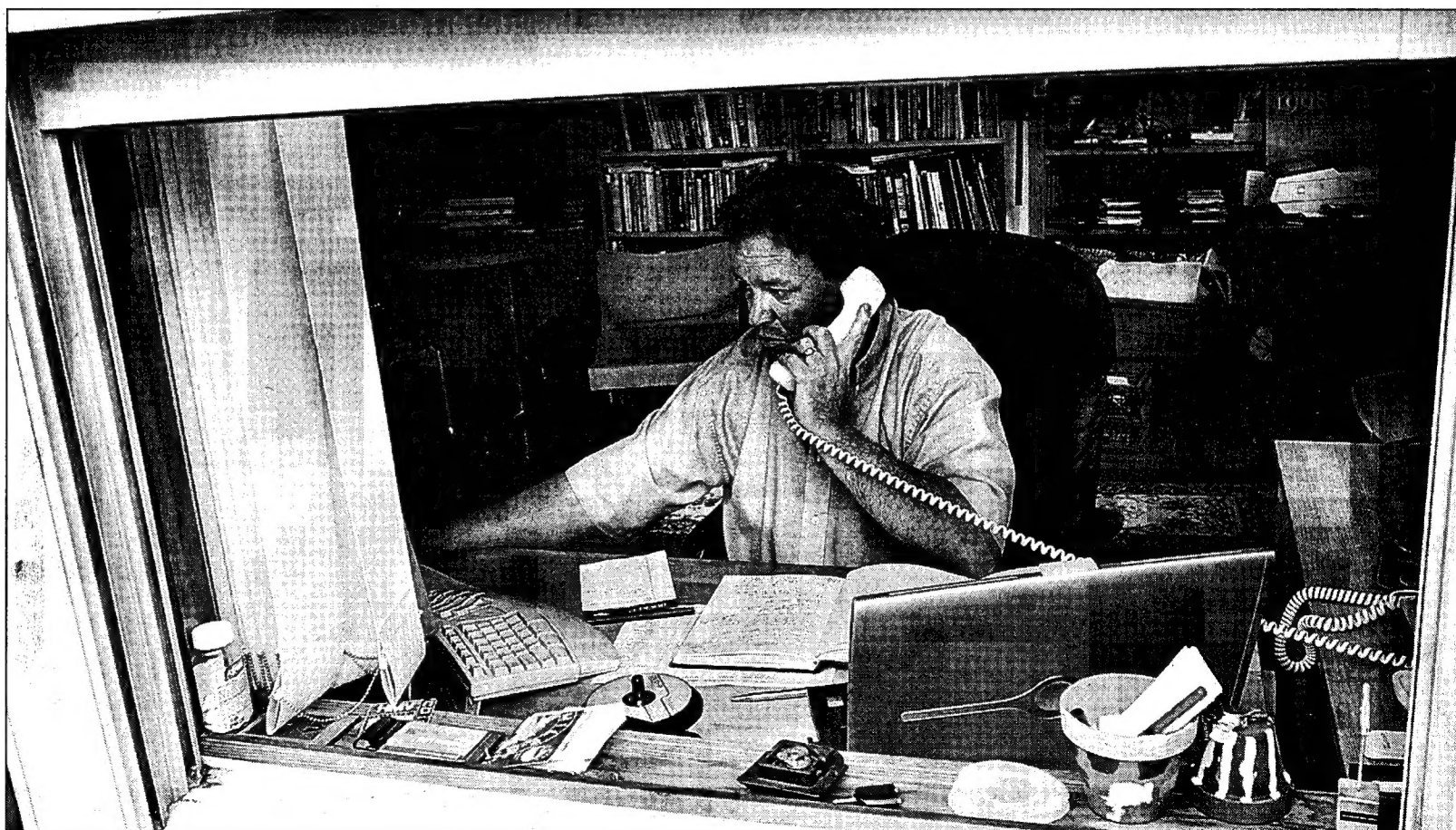
Huge bills can result from on-line breach

BY JACK KAPICA

Jim Carroll was stunned when Rogers Cable told him it had received a complaint that a hacker was using his Internet address.

Must be a mistake, he told Rogers, his Internet provider. Then a tech helper at the company walked him through his setup and discovered that indeed, he had inadvertently left his business Web server unprotected. It was what is called an "open relay." Someone found it, posted Mr. Carroll's address on more than 100 Russian bulletin boards, and soon hundreds of people were using Mr. Carroll's machine to surf anonymously.

Mr. Carroll thought he received the nice treatment from Rogers because he is a noted high-tech authority, public speaker and author of the book, *Surviving the Information Age*. But the Rogers support technician was just doing his job, a job that's becoming routine among larger Internet providers — policing subscribers who don't know their computers have been hijacked or hit with a virus that turns them either into open relays or spam-serving "zombie" machines.



J.P. MOCZULSKI/THE GLOBE AND MAIL

Noted high-tech authority Jim Carroll — shown in his home office — left his server unprotected and was victimized by on-line hackers.

A few weeks ago, Sympatico, the country's largest digital subscriber line (DSL) Internet provider, suspended the outbound mail service of more than 400 customers whose machines had been infected and were spewing spam. The customers were informed that service would not be restored until their machines were cleaned.

Tactics like this are becoming a necessity in a world where spammers and hackers are getting so sophisticated that ISPs cannot expect all their customers to know how to deal with them. And if a person as tech-savvy as Mr. Carroll had no idea his server had been compromised, how could individuals or small businesses without IT departments fare any better?

A few months ago, Mike Bierstock, who runs a tiny property management business in Waterloo, Ont., found his office system had been compromised — either by a virus or hacker, he's not sure — and he was slapped with a terrific bill for the volume of traffic generated by his computer. His access provider forgave some of his initial bills, but did nothing to help him clean his system, so the prob-

lem continued. Ultimately the ISP killed his account, hitting him with a bill of \$11,000.

Another subscriber to the same ISP, Isaac Liber, who runs a small high-tech company in Concord, Ont., was also the victim of a computer worm. The ISP handed him a bill for \$77,000, then raised it to \$85,000.

Mr. Liber simply declared bankruptcy. "They knew about the worm way before any billing had accumulated," said Mr. Liber, now senior account executive with iTel Solutions Inc. "They also confirmed that while they knew that there was a worm and that they knew it was not our doing, they [say] the responsibility is ours. Yet only they could have stopped the worm and the massive amount of bandwidth that was flowing through because of this worm."

In both cases the ISP declared that it does not look into what the subscribers are doing with their bandwidth; all that matters to them is the volume being used. While this sounds like the ISP is respecting privacy, it's really a hard-nosed business practice that places all the responsibility on the subscriber.

Mr. Liber and Mr. Bierstock were unlucky with their choice of ISP; most providers will simply write off the obviously fraudulent charges to keep their subscribers happy. Credit card companies do this routinely with people whose identities have been stolen, as do telephone companies with hacked lines.

But it's a new field for Internet access providers, especially since so much of the access business is based on billing for volume of use.

Tom Copeland, president of the Canadian Association of Internet Providers, says it is legal to bill customers for virus-related activity, such as hitting businesses with five-figure usage bills. "But I can't imagine that the ISP would have let the situation get to that point."

He also said that usually this kind of abrupt billing practice is found among business accounts and not with residential users, who are harder to bill for such large amounts. But residential users are no less vulnerable to the viruses that cause the problem.

Sympatico has started blocking outgoing e-mail from infected machines, said spokeswoman Nessa Prendergast, so they can still surf and receive e-mail until the prob-

lem is solved. Users get a message saying that Sympatico has taken that step, and if they can't clean up their machines themselves, they can call technical support and get help. "We clean them up, reset their computers and get them going again," she said.

Over at Rogers Cable, there's a full-time abuse team that tracks individual subscribers' Internet usage, said company spokeswoman Taanta Gupta. If it goes way up, it's usually a sign of an infected machine. And every time a new virus arrives, users "into the thousands" have to be told to clean their machines, she said.

It's Rogers' policy to send an e-mail warning to the infected machine's owner, and then provide telephone help to disinfect their systems. If a customer does not respond, Rogers will suspend the account — which usually gets a fast response from the customer, who, Ms. Gupta says, is in a much more receptive frame of mind about cleaning the machine at that point.

The ISP arm of Vancouver-based Telus Corp. also has an abuse team that starts by calling users of infected machines, said director of Internet services Blair Miller. The

team sends an e-mail laying out what the user must do to kill the infection.

"We get great traction off those e-mails," Mr. Miller said.

And, like most other large ISPs, Telus offers a free anti-virus service aimed at keeping the number of infections down. "We don't want to lose customers," he added.

So how do Internet users protect themselves?

First, users should read that tedious small print in the contract with an ISP. If it says there's a monthly limit on the amount of bandwidth you use and that you are solely responsible for all Internet activity, then look elsewhere for service.

Second, ask whether the ISP offers help for machines infected with a virus.

Finally, most ISPs say users must have proper anti-virus protection, including anti-virus software from a commercial vendor (such as McAfee or Symantec), or use a similar service supplied by the ISP. They should also make sure the anti-virus program is constantly up to date — most programs can be set to do this automatically — and that a full scan of the system be done frequently.